REMARKS

In view of the following remarks, Applicants respectfully request reconsideration and allowance of the subject application. Claims 6 and 7 are canceled without prejudice, Claims 8 and 9 are as originally filed, Claims 2-5, 10 and 16 were previously presented, and Claims 1, 11-15 and 17-21 are currently amended. Accordingly, Claims 1-5 and 8-21 are pending.

Claim Objections

Claim 14 is objected to because of an informality noted by the Examiner. Applicants have amended Claim 14 to make the noted correction.

Claim Rejection under 35 U.S.C. § 112

Claim 18 is rejected under 35 U.S.C 112 because there is insufficient antecedent basis for the limitation of "the first value" and "the threshold." Applicants have amended Claim 18 to correct the antecedent basis of the noted limitations.

Claim Rejection under 35 U.S.C. § 101

Claims 1-5 and 8-21 are rejected under 35 U.S.C 101 because the claims are non-tangible or are not limited to tangible embodiments. Applicants have amended Claims 1, 11-15 and 17-21 to limit the scope of the claims to tangible embodiments.

Claim Rejection under 35 U.S.C. § 102

Claims 1-5, 8-17 and 19-21 stand rejected under 35 U.S.C. § 102 as being anticipated by U.S. Patent No. 6,463,535 to Drews. Applicants respectfully traverse the rejection of Claims 1-5, 8-17 and 19-21. Drews discloses a technique for downloading a boot image to a local platform. The technique utilizes a signed manifest 150 transmitted with the boot image and an authorization certificate 280 stored on the local platform to verify the integrity of the downloaded boot image. The signed manifest 150 is also utilized to confirm that the boot image was received from an authorized source.

Claim 1, as amended, recites a method of associating a permission set with a code assembly based on evidence characterized by different levels of trust, the method implemented at least in part by a computing device that includes:

- identifying a first condition for association with the permission set, wherein the first condition references a first element of evidence, wherein the first element of evidence is implicitly trusted and **wherein the permission set is used to control operation of the code assembly during run-time;**
- identifying a second condition for association with the permission set, wherein the second condition references a second element of evidence, wherein the second element of evidence is initially untrusted;
- determining whether the first condition is satisfied by the first element of evidence;

- determining whether the second element of evidence should be trusted based on the first condition;
- determining whether the second condition is satisfied by the second element of evidence; and
- associating the permission set with the code assembly, if both the first condition and the second condition are satisfied.

Drews does not disclose "identifying a first condition for association with the permission set ... wherein the permission set is used to control operation of the code assembly during run-time" or "identifying a second condition for association with the permission set." Applicants cannot find any mention of a "permission set" in Drews. Furthermore, the Office has failed to identify what element in Drews is equivalent to "a permission set," and in particular a "permission set" that is "used to control operation of the code assembly during run-time."

Furthermore, Drews does not disclose "associating the permission set with the code assembly, if both the first condition and the second condition are satisfied." Instead, Drews discloses a signed manifest for use in performing an integrity check of the boot image and determining if the boot image has been provided by an acceptable source. In particular, the integrity check procedure verifies that the boot image has not been modified since the signed manifest 150 was created. Authorization to run the boot image (e.g., provided by an acceptable source) is determined by analyzing

the signed manifest 150 using the public key provided by the authorization certificate 280.

Determining whether the boot image is authorized to run on the local platform using the authorization certificate 280 and/or signed manifest 150 does not include "associating the permission set with the code assembly, if both the first condition and the second condition are satisfied" wherein "the permission set is used to control operation of the code assembly during run-time." For example, Drew does not disclose that the authorization certificate 280 and/or signed manifest 150 can affect control of whether a protected file can be read, whether a type checking operation can be skipped, and/or the like during run-time execution of the boot image. Thus, Drew only discloses determining if an application is authorized to run and not associating a permission set used to control operation of the code assembly when it is run.

For each of the reasons set forth above, Applicants respectfully submit that Claim 1 is patentable over Drews. Accordingly, Applicants request that the §102 rejection of Claim 1 be withdrawn and that Claim 1 be allowed.

Claims 2-5 and 8-10 are allowable by virtue of their dependency on respective base Claim 1, as well as the additional elements they recite. Accordingly, Applicants respectfully request that the §102 rejection of Claims 2-5 and 8-10 be withdrawn and that Claims 2-5 and 8-10 be allowed.

Claim 11, as amended, recites one or more computer-readable media having instructions that, when executed on one or more processors perform a process for

associating a permission set with a code assembly based on evidence characterized by different levels of trust that includes:

- generating a collection of code groups, **wherein each code group is used to define a category of related code assemblies**, each code group being associated with a membership criterion and **a permission set used to control operation of the code assembly during run-time**;
- receiving the membership criterion associated with one of the code groups, the membership criterion including at least a first condition and a second condition;
- referencing a first element of evidence in the first condition, wherein the first element of evidence is trusted independent of other evidence and conditions;
- referencing a second element of evidence in the second condition, wherein the second element of evidence is initially untrusted;
- determining whether the first condition is satisfied by the first element of evidence;
- determining whether the second element of evidence should be trusted based on the first condition;
- determining whether the second condition is satisfied by the second element of evidence;